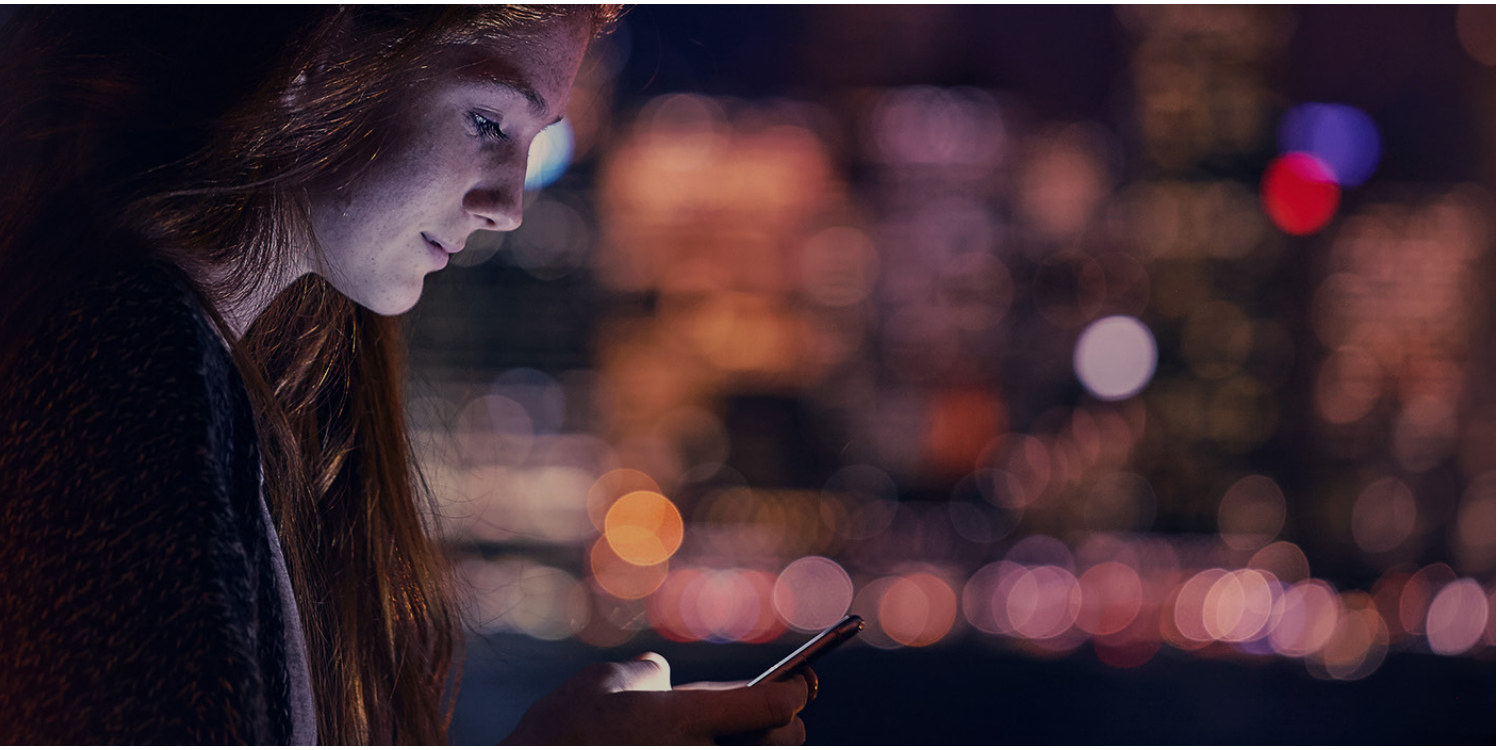
White Ops

Application Integrity

Megan Baker - VP, Customer Success

White Ops

White Ops **Application Integrity** protects against the abuse of applications and websites by sophisticated bots and fraudsters, including sensitive data scraping, new account fraud, and account takeover attacks. To defeat sophisticated bots, White Ops uses a multilayered detection methodology that isn't reliant on any single technique. This means we are able to detect and block today's dynamic and polymorphic bots, to ensure only real humans interact with your applications.



It has become more and more difficult for enterprises to distinguish customers from fraudsters in today's digital environment.

Even when applications function as intended, they are vulnerable to fraudsters who have compromised human identities to manipulate applications, businesses, and markets. Sophisticated bots - especially when they number in the millions and reside on residential devices - can mimic human behavior, such as mouse movements, keystrokes, and browser histories. Since these bots attacks look and act just like humans, they evade and overwhelm conventional detection methodologies.

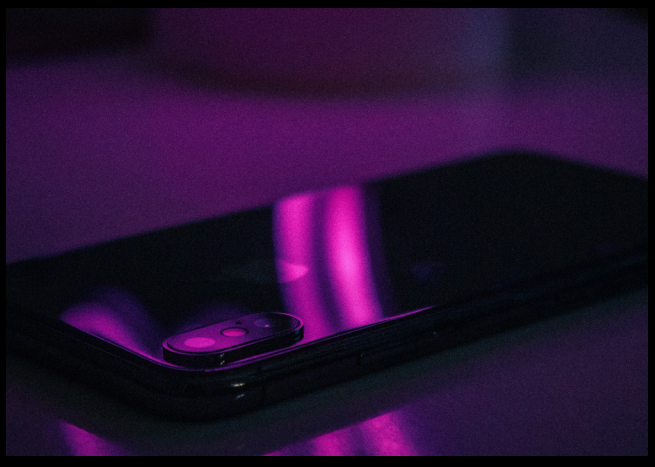
Use Cases

Account Takeover

White Ops mitigates the risk of account takeover attacks, including credential stuffing and credential cracking. Using our multilayered detection methodology, we detect signs of account takeover attacks without relying on any single technique, and prevent attacks outright. Our approach focuses on catching bots using technical evidence with the goal of minimizing impact to real users.

New Account Fraud

Criminals use bots to create accounts using the same process humans would. But since fraudsters can automate the process, they are able to create an immense number of accounts in a very short period of time. On certain platforms, this gives them the power to spam, post fake content, and skew the popularity of content native to your platform. White Ops identifies bots that attempt to go through the account creation process so you can prevent automated account creation and maintain the integrity of your applications.



Sensitive Data Scraping

White Ops makes it easy to detect and prevent automated scraping of high-value data including intellectual property and other paywall protected content. Fraud and Security teams can place White Ops detection tags to detect sensitive data scraping bots within minutes.

Benefits

Detect Even the Most Sophisticated, Dynamic Bots

We don't rely on any single technique to detect bots and automated threats. Instead, we use a combination of techniques, including gathering technical evidence of compromise, machine learning, global threat intelligence, and continuous adaptation. Our multilayered detection means we can detect malicious traffic, even in low signal environments. We can also separate malicious traffic from valid traffic originating from the same IP address.

Maintain Your User Experience with Minimal Impact on End Users

White Ops is able to detect bots and automated threats without needing to collect invasive information. Moreover, once our technology is integrated, there is minimal impact on anyone's experience on the web.

Gain Full Transparency into Each Detection

Other bot detection solutions provide little context into what they've detected and how. White Ops provides specific behavior on the threat category and the specific threat factors observed for each detection.

How Application Integrity Protects Against Sophisticated Bot Attacks

Passive Detection provides near real-time visibility and monitoring of malicious bot traffic occurring on your website and applications.

1. Place White Ops Detection tags:

White Ops detection tags are deployed within minutes via JavaScript or Software Development Kits (SDKs) for mobile applications. Our detection tags fire asynchronously and execute in the background with no impact to site load time or performance. Tags can be placed on log-in, account creation, password reset, or any other website pages or forms you need to protect.

2. Bring Your Own Signal:

Depending on the use case, your signal will improve detection capabilities, and also help identify instances of tag evasion.

3. Get Alerted to Malicious Traffic:

White Ops will report back malicious bot traffic detected to client systems (such as a SIEM or business intelligence platform) via API.

4. Report & Analyze:

The White Ops Dashboard and Reporting API allows for analysis of aggregate trends, custom reporting, and visualizations to understand fraud trends over time.

White Ops Bot Mitigation Platform

Collect Signals
Signal Evasion
Custom Data
Network
Device

Decision Engine

Classify Events
Bot
Nonstandard
Valid

Technical Evidence

Continuous Adaptation

Global Threat Intelligence

Machine Learning

JavaScript or SDK

Client

Allow - Delay - Block - Deceive

Server Integration

Mitigation

Application Integrity
Architecture and Implementation

1B+ detection events each day

300M devices observed each day

2,500 signals per detection

How White Ops is Different

Multilayered Detection Methodology

- Over 2500 signals involved each detection on average
- Granular visibility: we can distinguish bot from human activity on the same device

Visibility

- Each day, we see an average of 300 million unique devices
- More than 1 Billion interactions are observed using our detection payload each day

Global threat intelligence

- Our team proactively hunts and attributes ATO threat models
- Findings constantly feed our detection engine with new algorithms and updates
- We've driven efforts in major botnet takedowns such as Methbot and 3VE

Continuous adaptation

- We've been adapting our detection techniques for 7+ years, allowing us to stay ahead of the adversary more than other solutions that are built on fixed detection mechanisms

Active Prevention

Active Prevention enables real-time mitigation of malicious bots or nonstandard traffic. This allows your systems to take direct action (block, mark for review, deceive, etc.) as the request is occurring. Clients would implement this via direct server to server integration. When White Ops detects malicious traffic (such as known Account Takeover bots), you can invalidate the request to prevent any malicious logins or account creations from taking place.

Bot
2.6K
8.11%

Nonstandart
1.5K
4.47%

Valid
28.3K
87.14%

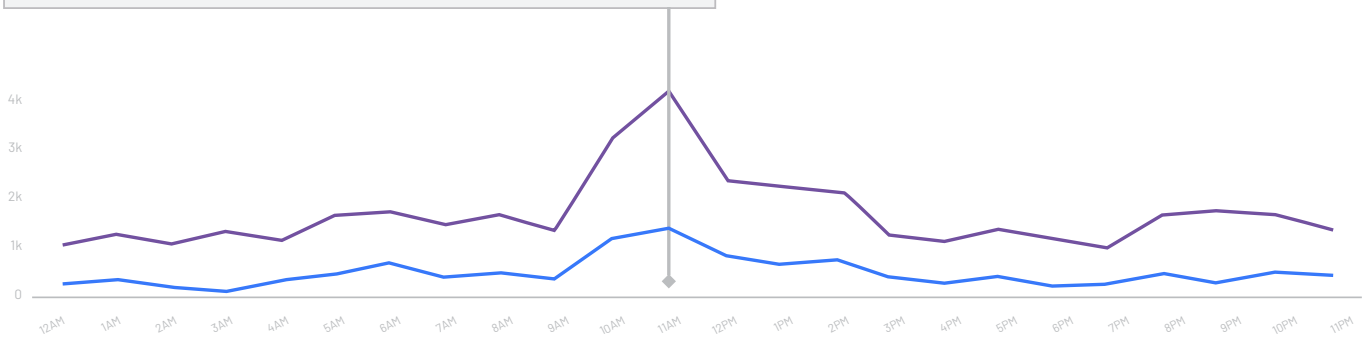
Blocked
2.6K
8.11%

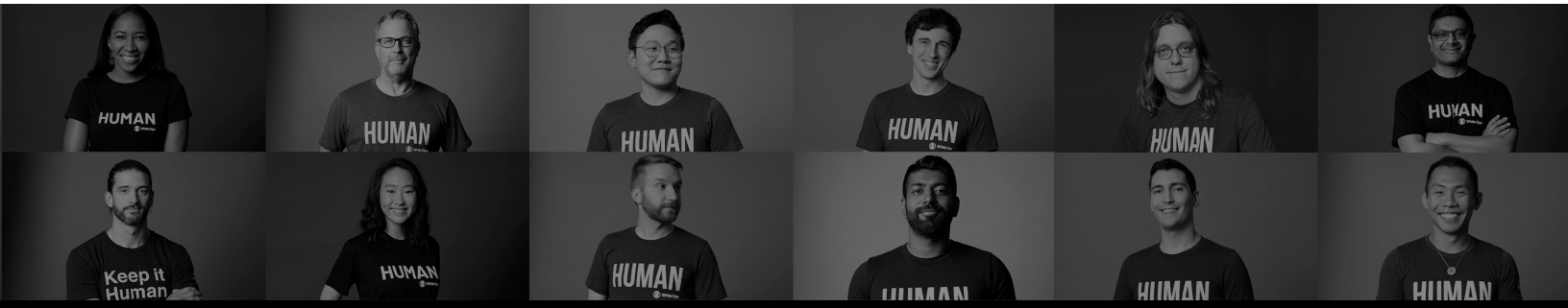
Allowed
29.5K
91.89%

Desktop	Mobile Web
55.3%	40.39%
18.3K	13.8K

Oct 11, 2019 11:00 AM	US/Eastern	
Total Events	9,699	30.60%
Bot	3,864	39.84%
Nonstandart	945	9.74%
Valid	4,890	50.42%

The White Ops Application Integrity Dashboard provides the specific threat category and factors observed for each detection event.





About Us

White Ops is the global leader in bot mitigation. We protect more than 200 enterprises—including the largest internet platforms—from sophisticated bots by verifying the humanity of nearly one trillion online interactions every week. The most sophisticated bots look and act like humans when they click on ads, visit websites, fill out forms, take over accounts, and commit payment fraud. We stop them.
To learn more about White Ops, visit **www.whiteops.com.**

www.whiteops.com

Keep it Human

White Ops